Director Platform Specifications

- HP, SPARC
- IBM workstation (in process)

Supported Operating Systems

- HP O/S 10.10 and higher
- Solaris 2.4 and higher
- IBM AIX 4.1 and higher

Hardware Specifications

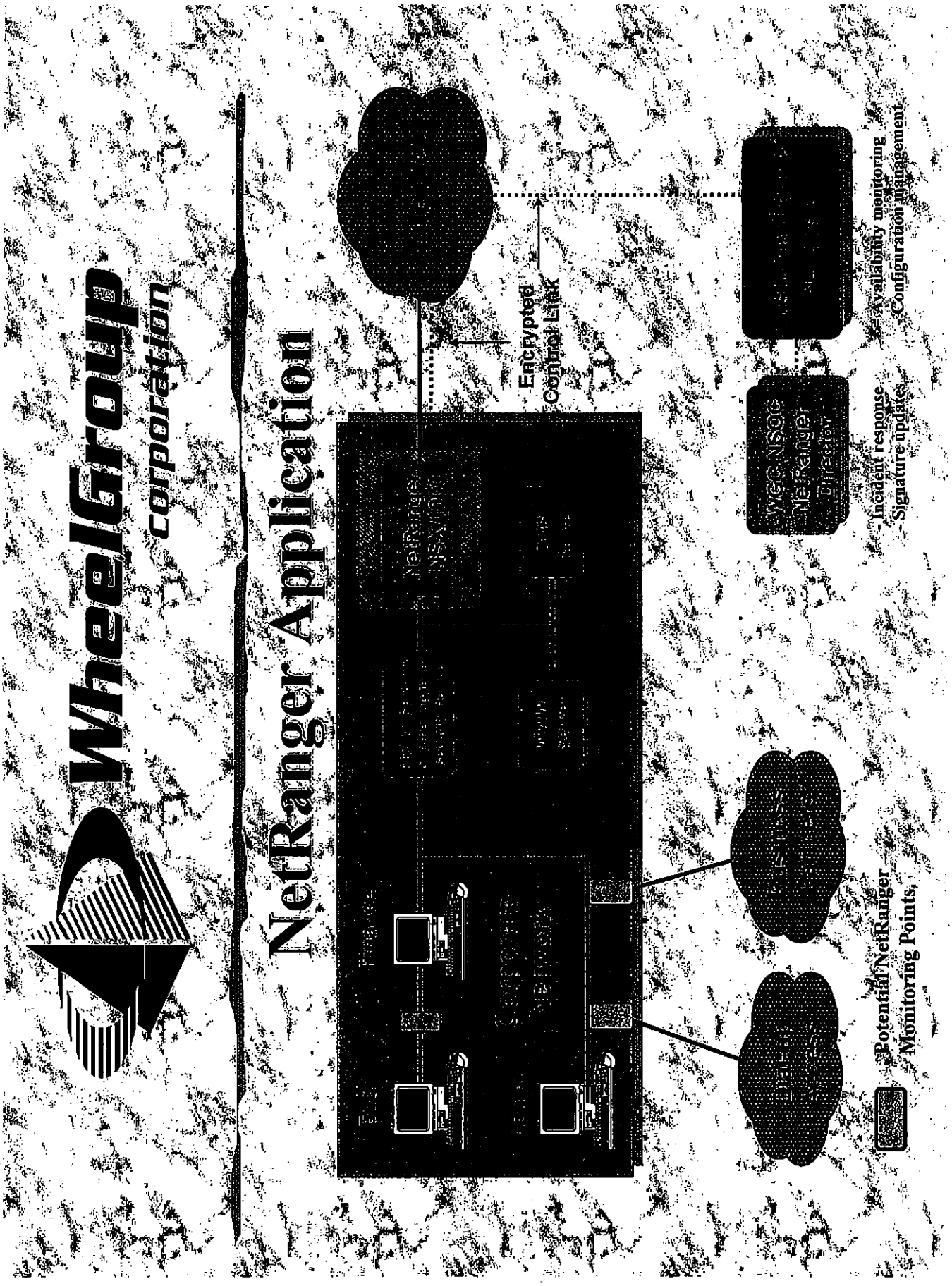
- minimum 96 MB RAM
- minimum 4 GB SCSI hard drive
- 20" Color monitor

Director Platform Specifications (cont.)

- Network management platforms
  - HP OpenView or IBM NetView
- Database interface
  - Oracle SQL *Net
  - Remedy
- GUI configuration interface
  - Java

WheelGroup
corporation
Communication Architecture
Flexible
Fault Tolerant
Secure
Scaleable
NSX
NSX
NSX
NSX
NSX
Director
Director
Director

WheelGroup
corporation
Operational Overview
customer site
ISP or carrier
WAN connection
Internet
(or other WAN)
Host "A"
Ether
NSX
BG
Customer
LAN
filter info & commands
NetRanger
M/C SVPN
config info
& alarms
Host "B"
NSX IDS
processor
NetRanger
Director
Types of attacks detected
Context - SATAN probes, port & ping sweeps, etc
Content - sendmail, loadmodule, org. policy violations, etc.
Event levels
1) info only - call detail records, etc
2) admin - policy violations, configs etc
3) alarm - minor security violation
4) alarm - major security violation
5) alarm - attack in progress


WheelGroup
corporation
NetRanger Application
Encrypted
Control Link
VYGC NSOC
NetRanger
Director
Availability monitoring
Configuration management
Incident response
Signature updates
Potential NetRanger
Monitoring Points

WheelGroup
corporation
Distributed Network Security Management
Enterprise
Strategic
Management
Regional
Operational
Management
Local Network
Security
Management
Director
Tier 1
Director
Tier 2
Director
Tier 3
Director
Tier 3

WheelGroup
corporation
NetRanger NSX
Expert system
Real-time intrusion detection and instantaneous "surgical" response
Content and Context monitoring
Redundant, robust, communications architecture for assured event notification
Secure VPN
56k, T1/E1, Ethernet, T3, 100Mbps
Plug-n-play
Sun (SPARC & PC), HP, IBM

WheelGroup corporation

NetRanger NSX Alarm Levels

Alarm Level	Network Config Events	Network Usage Events	Network Security Events
LEVEL 0	Misc Ignored Ports	Misc Ignored Ports	
LEVEL 1	Misc Network Traffic	Packets From Tracked Services	
LEVEL 2	Misc Failed Packets	Packets Travelling to Blocked Sites	Authentication tcp P 113
LEVEL 3			Failed DNS Attempts Failed SMTP Attempts Failed FTP Attempts Failed Telnet Attempts Failed X Session Attempts Failed Finger Attempts
LEVEL 4	Lost Heartbeat Router Interface Down Failed NSX		Failed SNMP Attempts Failed RPC Attempts Failed TFTP Attempts Failed Rsh Attempt Failed Rlogin Attempt Failed Rexec Attempt Login To Router Password Change On Router
LEVEL 5			Sendmail w/ "from: |tail IFS=/ Port Sweeping (tcp/udp) ICMP Sweeping Source Routing IP Spoofing Fragmented TCP Headers SATAN Attack
LEVEL 6			Multiple Hacking Attempts

WheelGroup
corporation
NetRanger Director
Point & click GUI
"On the fly" remote NSX configuration control
Open systems (HP OpenView, NetView, Oracle)
Real-time ICON alarm notification
Interpretive incident reporting
Misuse auditing
Reports (audits, trends, incidents, usage)
Sun, HP, IBM

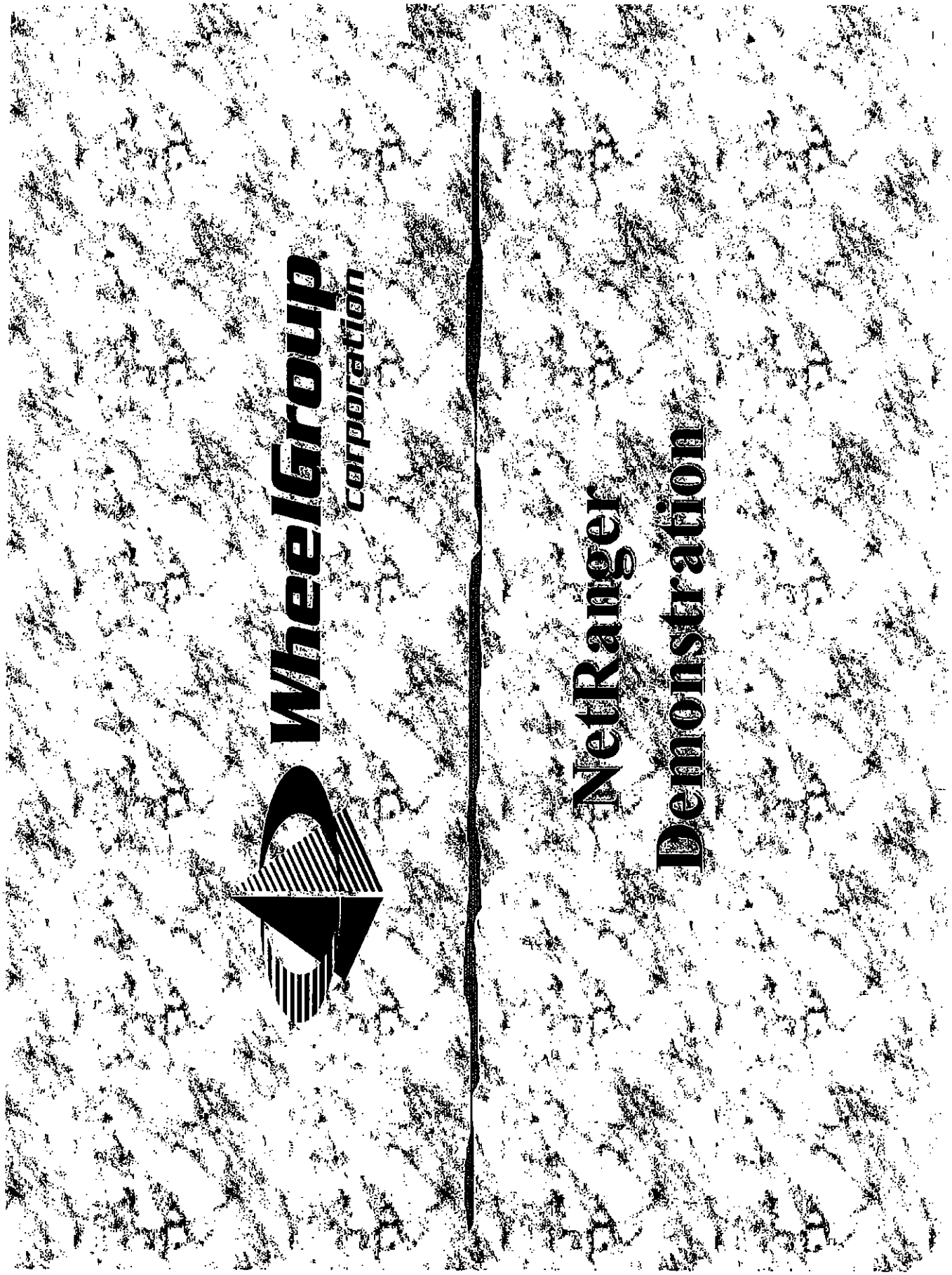
NetRanger Director Monitoring GUI
WheelGroup
corporation
RootMap
IBM
North Carolina
NSX-2000
NSOC
US Air Force
NSX-2000
IBM
US Air Force
North Carolina

WheelGroup
corporation
NetRanger Director Alarm GUI
SATAN attack!
ping Sweep
Found ++
RootMap
Security
Secure Shell
North Carolina

WheelGroup corporation

Hardware Specifications

- NSX Sensor
  - 7" high
  - 19" wide (including rabbit ears)
  - 20" deep (including rabbit ears)
  - weighs 32 pounds
- BorderGuard 1000
  - 2" high
  - 10" wide (including rabbit ears)
  - 17.5" deep
  - weighs 15 pounds
- BorderGuard 2000
  - 6.5" high
  - 19" wide
  - 17.5 deep
  - weighs 25 pounds


WheelGroup
Corporation
NetRanger
Demonstration

NetRanger Pre-Installation Considerations

Wheelgroup Corporation

Analyze Current Network Architecture

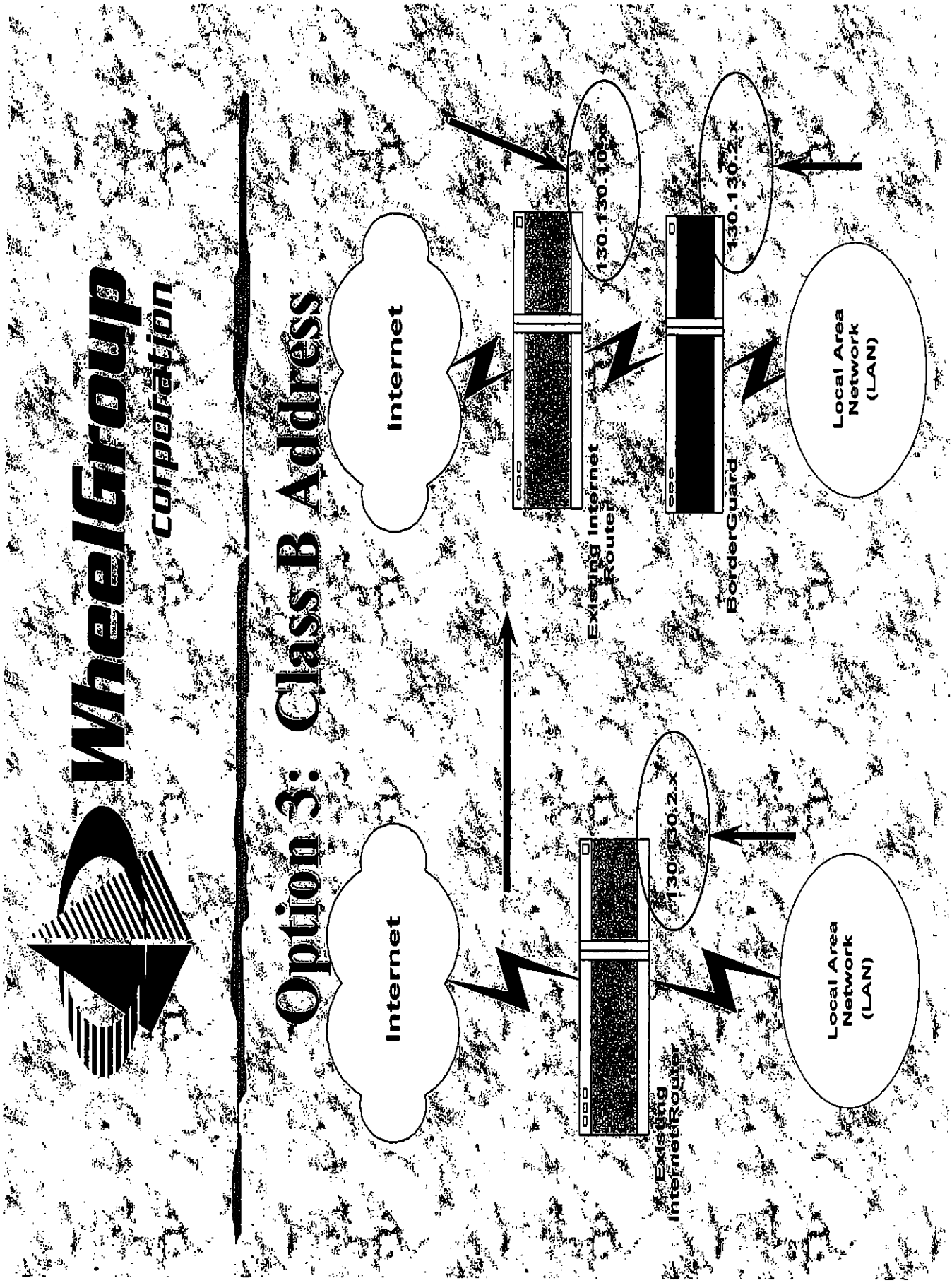
- Identify what to protect.
  - Internet
  - Remote sites
  - Business partners
  - Departments
- Define all entry and exit points to the protected network.
  - One geographic location, no existing internet connections
  - One geographic location, existing internet connections
  - Multiple geographic locations, existing internet connections
- Identify current security measures.
  - Existing Firewalls
  - Security Filters

WheelGroup
corporation
Option 1: Install the BorderGuard as a Bridge
Internet
Existing Internet Router
193.20.20.x
BorderGuard
Local Area Network (LAN)

WheelGroup
corporation
Option 2: Install the BorderGuard as
an Internet Router
Internet
BorderGuard
Local Area
Network
(LAN)

Options 3-6: Unable to Replace Existing Router

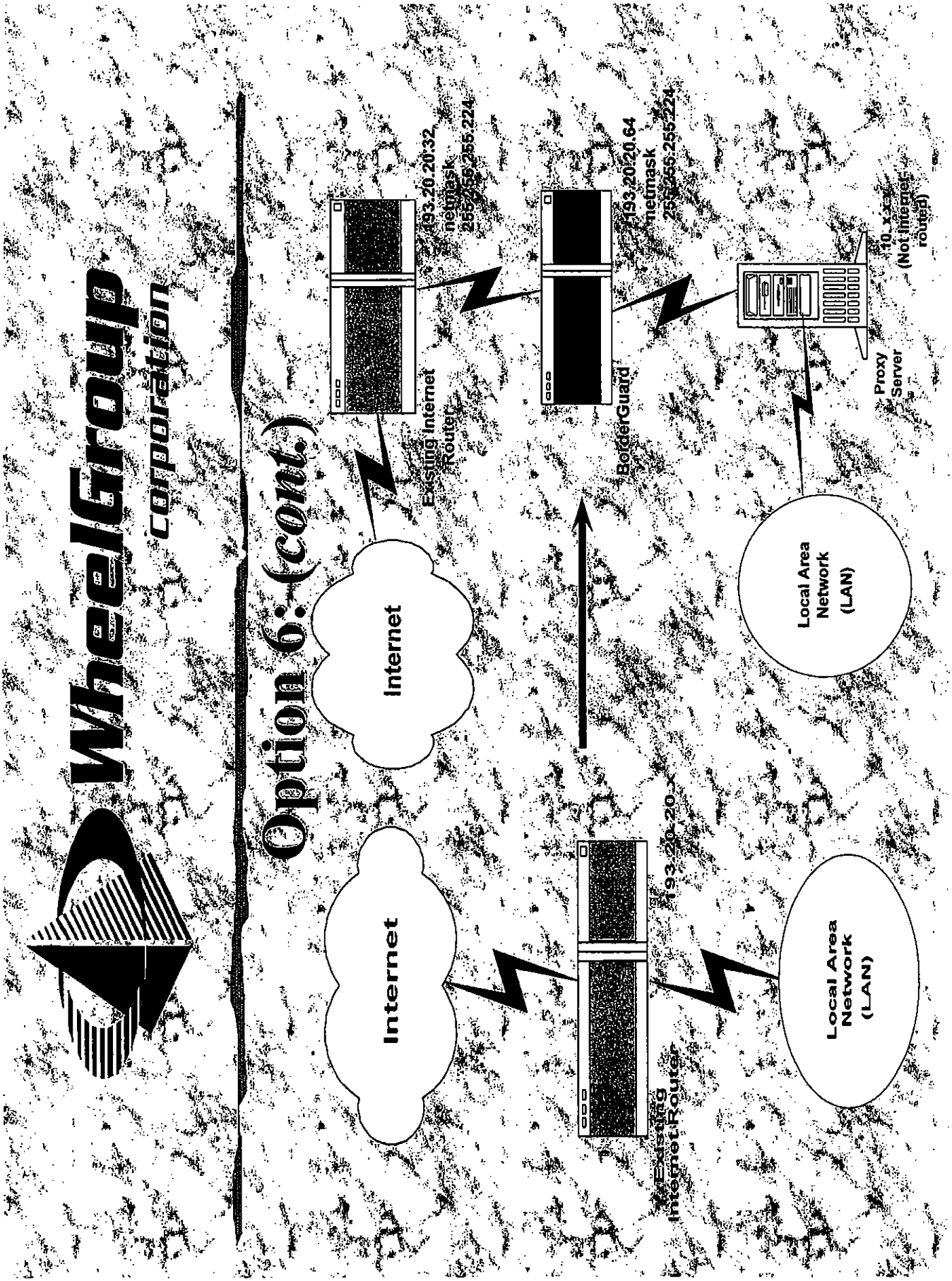
- Class B Address
- One or more Unused Class C Addresses
- No Unused Class C Addresses
- Class C Address that Cannot be Subnetted


WheelGroup
corporation
Option 3: Class B Address
Internet
Existing Internet Router
130.130.10.x
BorderGuard
130.130.2.x
Local Area Network (LAN)
Internet
Existing Internet Router
130.130.2.x
Local Area Network (LAN)

WheelGroup
corporation
Option 4: An Unused Class C Address
Internet
Existing Internet Router
193.20.21.x
BorderGuard
193.20.20.x
Local Area Network (LAN)
Internet
Existing Internet Router
193.20.20.x
Local Area Network (LAN)

WheelGroup
Corporation
Option 5: No Unused Class C Addresses
Internet
Existing Internet Router
193.20.20.32
netmask
255.255.255.224
BorderGuard
193.20.20.64
netmask
255.255.255.224
Local Area Network (LAN)
Internet
Existing Internet Router
193.20.20.x
Local Area Network (LAN)

WheelGroup
corporation
Option 6: Unable to Subnet Existing Class C Address
Internet
Existing Internet Router
198.15.44.x (New Class C)
BorderGuard
193.20.20.x
Local Area Network (LAN)
Internet
Existing Internet Router
193.20.20.x
Local Area Network (LAN)


WheelGroup corporation
Option 6: (cont.)
Internet
Existing Internet Router
193.20.20.32
netmask
255.255.255.224
Internet
Existing Internet Router
193.20.20.x
BorderGuard
193.20.20.64
netmask
255.255.255.224
Local Area Network (LAN)
Proxy Server
10.x.x.x
(Not internet routed)
Local Area Network (LAN)

NetRanger NSX Sensor Installation Options

- Install the NSX Sensor on a Separate, Isolated Network
  - Most Secure NSX Connection
  - Only with the NSX 2000 or 5000
- Install the NSX Sensor on the Corporate Network
  - Can be used with NSX 1000, 2000 or 5000
- Install the NSX Sensor on a Switched Ethernet Network
  - Can be used with NSX 1000, 1000 or 5000

WheelGroup
Corporation
NSX Sensor on a Separate, Isolated Network
Internet
BorderGuard
NSX Sensor
Corporate Network

WheelGroup
corporation
Install the NSX Sensor on the
Corporate Network
Internet
BorderGuard
Corporate
Network
NSX Sensor